

REMARKS

In response to the Office Action dated April 15, 2005, Applicant respectfully requests reconsideration of the current rejections of the claims. The withdrawal of a number of the previous grounds of rejection, and objections, is noted with appreciation.

Although the rejection of claim 5 under 35 U.S.C. §112 was not repeated, the most recent Office Action states that the amendment to claim 5 is considered to be inadequate, in that the term "candidates" is not understood. To remove this issue, claim 5 has been amended to delete the term "as candidates."

Claim 9 was rejected under the second paragraph of 35 U.S.C. §112, as being indefinite. The basis for this rejection is not understood. In paragraph 17, the Office Action quotes the preamble of claim 9, and then states "the purpose of the limitation (above) is not understood...." The preamble of claim 9 is not intended to serve as a limitation. Claim 9 is a dependent claim, and pursuant to the requirements of 37 C.F.R. §1.75(c) comprises two parts, which respectively refer back to and further limit another claim in the application. The preamble, namely the recitation "the portable electronic device of claim 6" comprises the portion of the claim that refers back to another claim. The remainder of the claim, beginning with the "wherein" statement, comprises the portion that further limits the subject matter of claim 6. Specifically, claim 9 recites an additional function that is performed by the arithmetic processor defined in claim 6, namely the generation of a pair of cryptographic keys from the integers a, b.

The Office Action does not indicate why claim 9 is considered to be indefinite under the requirements of 35 U.S.C. §112, second paragraph. If the rejection is

maintained, the Examiner is respectfully requested to explain the basis therefore, so that Applicant will be apprised of any amendments that may be necessary to overcome the rejection.

The Office Action maintains the rejection of claims 1-6 under 35 U.S.C. §103, on the basis of the Lidl et al. publication in view of the prior art described in the application and the Schneier publication. Claims 6-9 were also rejected under 35 U.S.C. §103 on the basis of this prior art, in further view of the Murphy et al. patent. For the reasons presented in the previous response, and as further discussed below, Applicant respectfully submits that the claimed subject matter is not suggested by this prior art.

The cited pages of the Lidl et al. publication pertain to the RSA public-key cryptosystem. At page 290, the publication provides a definition of the Carmichael function $\lambda(n)$, which is a classical object in number theory. The main property of this function is set forth on page 291. This property states that, for any two numbers a and n , raising a to some power k , or to some other power $k' = k + "a multiple of" \lambda(n)$, will yield the same result, modulo n , as long as k is different from 0 and n is not divisible by a $(k+1)$ th power. This is a classical, well known property.

The claimed invention exploits a different property of the Carmichael function which, in a sense, corresponds to the case $k=0$ that is excluded by the above-stated property. The invention is based on the proposition that raising any number a to the power $\lambda(n)$, modulo n , yields a value of 1 if, and only if, the number a is co-prime to n . This is a different property from the one described above, and in the Lidl et al. publication.

The objective of the invention is, for some number n given together with $\lambda(n)$, to randomly select a number a from among all the numbers that are co-prime to n . In accordance with this objective, successive random values are generated and checked for co-primality with n by using the second property of the Carmichael function as the test for co-primality. It is respectfully submitted that this claimed feature is not suggested by the prior art of references.

The rejection of the claims notes that the Lidl et al. publication discloses the property $a^{\lambda(n)} = 1 \pmod{n}$. What the reference does not teach, however, is that this property can be used to determine whether n is co-prime to a . The previous Office Action acknowledged that the Lidl patent does not contain such a teaching.

The rejection relies upon the prior art described in the specification, as well as the Schneier publication, to show that it is known to test for co-primality between two randomly chosen numbers. However, neither these examples of the prior art, nor the Lidl et al. publication, teach the *specific* test that is recited in the claims. The Applicant is not attempting to claim the Carmichael function, *per se*, nor the general concept of testing for co-primality when selecting numbers to be used for cryptographic keys. Rather, the claims are directed to a *particular* test that is based upon the second noted property of the Carmichael function.

It is respectfully submitted that the cited prior art references do not disclose this claimed subject matter, whether considered individually or in combination. The prior art described in the specification and the Schneier publication disclose the desirability of testing for co-primality. However, they do not disclose a test that is based upon a property of the Carmichael function. The Lidl et al. publication describes the Carmichael function. However, it does not disclose that a particular

property of that function can be used as the test for co-primality. Consequently, there is no teaching in any of the references which leads a person of ordinary skill in the art to utilize the claimed property of the Carmichael function as a test for co-primality when selecting pairs of numbers to be used for the generation of cryptographic keys. Only Applicant's disclosure teaches this concept.

In summary, it is respectfully submitted that the combined teachings of the references do not suggest the steps of calculating the modular exponentiation $a^{b(b)}$ mod b, verifying whether this modular exponentiation equals 1 (to determine whether the integers a and b are co-prime), and generating cryptographic keys from the integers a and b when the equality is verified, as recited in claims 1 and 5. Similarly, they do not disclose a portable electronic device that performs these steps, as recited in claims 6-9.

Reconsideration and withdrawal of the rejections, and allowance of all pending claims are respectfully requested.

Respectfully submitted,

BURNS, DOANE, SWECKER & MATHIS, L.L.P.

Date: September 15, 2005

By: 
James A. LaBarre
Registration No. 28,632

P.O. Box 1404
Alexandria, Virginia 22313-1404
(703) 836-6620